SECTION II—CLAIMS

1. (Previously Presented) A method, comprising:

receiving a request including an address, the address comprising an address of a secure server with an address of a web page concatenated thereto, and the address being at least partially encrypted;

retrieving the web page designated in the request;

modifying an address associated with the retrieved web page to indicate an address associated with the secure server that retrieved the web page; and

encrypting data associated with the retrieved web page and sending, via a secure link, the encrypted data to a terminal that sent the request.

2. (Original) The method of claim 1 wherein the secure link comprises a secure sockets layer (SSL) link.

3. (Original) The method of claim 1 wherein modifying the address associated with the retrieved web page comprises modifying a Uniform Resource Locator (URL) or Internet Protocol (IP) address of a source web site that originated the web page.

4. (Original) The method of claim 1 wherein modifying the address associated with the retrieved web page comprises modifying an address associated with a hypertext link in the retrieved web page to indicate the address associated with the secure server.

5. (Original) The method of claim 1, further comprising modifying computer code associated with the retrieved web page to cause subsequent requests related to the retrieved web page to be sent to the secure server instead of to a source web site that originated the web page.

6. (Previously Presented) The method of claim 1, further comprising decrypting the address associated with the web page from an address received along with the request from the terminal.

7. (Original) The method of claim 1, further comprising repeating the retrieving, modifying, encrypting, and sending while the secure link is active.

8. (Original) The method of claim 1, further comprising triggering a deletion of stored electronic files at the terminal related to a communication via the secure link, in response to termination of the communication.

9. (Original) The method of claim 1, further comprising, at the secure server, controlling transmission of electronic files to the terminal based on preferences received from the terminal.

10. (Original) The method of claim 1, further comprising:

providing an intermediate unit to receive the request from the terminal;

at the secure server, receiving the request, forwarded from the intermediate unit;

retrieving the web page designated in the request from a source;

modifying address information in the retrieved web page to indicate a source address corresponding to an address of the intermediate unit rather than to an address of the source that provided the web page; and

directly sending an encrypted version of the retrieved web page from the secure sever to the terminal, via the secure link.

11. (Original) The method of claim 10, further comprising receiving, at the secure server, communication protocol information related to a communication between the terminal and the intermediate unit, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

12. (Original) The method of claim 10, further comprising receiving subsequent requests from the terminal at the intermediate unit rather than directly at the secure server from the terminal.

13. (Original) The method of claim 1, further comprising storing under a pseudonym at a location communicatively coupled to the secure server, electronic files sent from a web site along with the web page.

14. (Original) The method of claim 1, further comprising:

obtaining information related to a user's communication with the secure server;

providing the obtained information to an entity based on permission of the user and in exchange for providing the secure link; and

providing advertisements from the entity to the user related to the obtained information.

15. (Original) The method of claim 1, further comprising:

providing a viewing window at the terminal;

displaying the retrieved web page at the viewing window; and

providing an interface for subsequent communication with the secure server from the viewing window.

16. (Previously Presented) A method, comprising:

providing an intermediate unit to receive a request for a web page from a terminal, the request including an address comprising an address of a secure server with an address of a web page concatenated thereto, and the address being at least partially encrypted;

at a secure server, receiving the request, forwarded from the intermediate unit;

retrieving the web page designated in the request from a source;

modifying address information in the retrieved web page to indicate a source address corresponding to an address associated with the intermediate unit rather than to an address associated with a source that provided the web page; and

directly sending an encrypted version of the retrieved web page from the secure server to the terminal, via a secure link.

17. (Original) The method of claim 16, further comprising receiving, at the secure server, communication protocol information related to a communication between the terminal and the intermediate unit, to allow the secure server to respond to requests sent to the intermediate unit from the terminal.

18. (Original) The method of claim 16 further comprising receiving subsequent requests from the terminal at the intermediate unit rather than directly at the secure server from the terminal.

19. (Original) The method of claim 16, further comprising:

receiving from the intermediate unit and at the secure server, encrypted address information associated with the web page, concatenated with the address associated with the intermediate unit;

decrypting the encrypted address information and retrieving a web page corresponding thereto; and

re-encrypting the address associated with the retrieved web page and concatenating the re-encrypted address with the address associated with the intermediate unit.

20. (Previously Presented) A machine-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to effect the following:

receive a request including an address, the address comprising an address of a secure server with an address of a web page concatenated thereto, and the address being at least partially encrypted;

responsive to the request, retrieve a web page designated in the request;

modify an address associated with the retrieved web page to indicate an address associated with the secure server that retrieved the web page; and

encrypt data associated with the retrieved web page and send, via a secure link, the encrypted data to a terminal that sent the request.

21. (Original) The machine-readable medium of claim 20 wherein the instructions cause the processor to effect the following:

send the encrypted data via the secure link by sending the encrypted data via a secure dockets layer (SSL) link.

22. (Original) The machine-readable medium of claim 20 wherein the instructions cause the processor to effect the following:

modify the address associated with the retrieved web page by modifying a Uniform Resource Locator (URL) or Internet Protocol (IP) address of a source web site that originated the web page.

23. (Original) The machine-readable medium of claim 20 wherein the instructions cause the processor to effect the following:

receive the request from the terminal forwarded from an intermediate unit;

retrieve the web page designated in the request from a source;

modify address information in the retrieved web page to indicate a source address corresponding to an address associated with the intermediate unit rather than to an address associated with the source that provided the web page; and

directly send an encrypted version of the retrieved web page from the secure server to the terminal, via the source link.

24. (Previously Presented) A machine-readable medium having stored thereon instructions, which when executed by a processor cause the processor to effect the following:

receive a request for a web page from a terminal, the request including an address, the address comprising an address of a secure server with an address of a web page concatenated thereto, and the address being at least partially encrypted; and

forward the request from the terminal to the secure server to allow the secure server to retrieve the web page designated in the request from a source and to allow the secure server to directly send an encrypted version of the retrieved web page from the secure server to the terminal, via a secure link.

25. (Original) The machine-readable medium of claim 24 wherein the instructions further cause the processor to effect the following:

send to the secure server communication protocol information related to a communication with the terminal, to allow the secure server to respond to requests sent from the terminal.

26. (Original) The machine-readable medium of claim 24 wherein the instructions further cause the processor to effect the following:

receive subsequent requests from directly the terminal rather than directly at the secure server.

27. (Original) The machine-readable medium of claim 24 wherein the instructions further cause the processor to effect the following:

receive an encrypted address concatenated with other address information via a secure connection;

decrypt the encrypted address and retrieve an address associated with the secure server or the address associated with the web page therefrom; and

send the request to the decrypted address.

28. (Previously Presented) An apparatus, comprising:

a processor coupled to a storage unit, the storage unit being capable of storing a computer program; and

a communication unit to allow the processor to communicate with a terminal and with a web site, wherein responsive to a request from the terminal including an address comprising an address of a secure server with an address of a web page concatenated thereto, the address being at least partially encrypted, the processor is capable of effecting execution of the computer program to retrieve a requested web page from the web site via the communication unit, to modify an address of the retrieved web page to a different address, to encrypt data associated with the retrieved web page, and to send the encrypted data to the terminal via a secure link communicatively coupleable to the communication unit.

29. (Original) The apparatus of claim 28 wherein the secure link comprises a secure sockets layer (SSL) link.

30. (Original) The apparatus of claim 28, further comprising a database unit communicatively coupled to the processor to store electronic files under a pseudonym, the electronic files corresponding to data sent from the web site along with the retrieved web page.

31.-33. (Canceled)

34. (Previously Presented) A system, comprising:

a server communicatively coupleable to a network and to a terminal, the server being capable of sending data from the network to the terminal in an encrypted form via a secure link, in response to a request received from the terminal, the request including an address comprising an address of a secure server with an address of a web page concatenated thereto, the address being at least partially encrypted, wherein the data sent to the terminal indicates the server as a source of the data; and

an intermediate unit communicatively coupleable to the server, the server being capable of receiving the request from the terminal via the intermediate unit and sending the data responsive to the request directly to the terminal via the secure link.

35. (Original) The system of claim 34 wherein the secure link comprises a secure sockets layer (SSL) link.

36. (Original) The system of claim 34 wherein the intermediate unit is capable of receiving subsequent requests from the terminal and sending the request to the server, the server being capable of receiving the requests from the intermediate unit and sending data responsive to the request directly to the terminal, the data sent to the terminal indicating a source address corresponding to the intermediate unit rather than an address corresponding to the server.